

SAM de validación

**BIT
Versión 2.92**

Título	SAM_Validación
Proyecto	542ce224-BIT-NOT-RES-CTM-AIT
Versión	2.92
Autores	Amor León y Luis Criado

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

Control de versiones

Versión	Descripción	Fecha
1.0	Documento original	
1.2	Aclaración de la obtención de las Claves de Sesión	17-04-2006
1.3	Comando de firma	20-06-2006
2.0	Se han eliminado los comandos que no se usan en validación. Se ha añadido una explicación del proceso de autenticación y un epígrafe de preguntas frecuentes	30-06-2006
2.1	Añadido: limitación el SAM con los comandos PPS	24-07-2006
2.2	¿Que claves hay que utilizar en la SAM de Validación?	28-08-2006
2.3	Correcciones generales	02-01-2007
2.4	Retrocompatibilidad SAM tipo 4, epígrafe 1.7	03-05-2017
2.5	Retrocompatibilidad SAM tipo 4, epígrafe 1.7 errata ID	04-10-2017
2.6	errata pag 9, arranque SAM por defecto	04-10-2017
2.7	Se han añadido los puntos 1.5.3 y 1.5.4, que se corresponden al a autenticación con diversificación NXP (2TDEA), según la nota de NXP AN10922, capítulo 2.4 2TDEA key https://www.nxp.com/docs/en/application-note/AN10922.pdf	02-02-2018
2.8	Ejemplo 5 del epígrafe 1.7.1. Selección de claves para tarjeta virtual	04-06-2018
2.9	Asignación de KeySet para tarjetas virtuales del CRTM	04-07-2018
2.91	Corregido valor del parámetro P2 del apartado 1.2. SELECCIÓN DE APLICACIÓN	31-10-2018
2.92	Explicación uso de claves de Validación en SAM tipo 4 ver 2 para setKey >1. Apartado de preguntas frecuentes “¿Qué claves hay que utilizar en el SAM de Validación y en la tarjeta DesFire?”	10/02/2021

INDICE

1. COMANDOS DEL MÓDULO SAM DE VALIDACIÓN.....	4
1.1. RESET.....	4
1.2. SELECCIÓN DE APLICACIÓN	4
1.3. VERIFICACIÓN PIN (PARA OBTENER CLAVE DE SESIÓN)	5
1.4. OBTENER RESPUESTA.....	5
1.5. OBTENCIÓN DE CLAVE DE SESIÓN	6
1.5.1. OBTENCIÓN DE CLAVE DE SESIÓN – Div. CRTM – 1ª parte.....	6
1.5.2. OBTENCIÓN DE CLAVE DE SESIÓN – Div. CRTM – 2ª parte.....	7
1.5.3. OBTENCIÓN DE CLAVE DE SESIÓN – Div. NXP 2TDEA – 1ª parte.....	8
1.5.4. OBTENCIÓN DE CLAVE DE SESIÓN – Div. NXP 2TDEA – 2ª parte.....	9
1.6. FIRMA DEL SAM	10
1.7. RETROCOMPATIBILIDAD CON LOS SAM DE TIPO 4	11
1.7.1. SELECT_KEYSET (instrucción 47h).....	12
2. PREGUNTAS FRECUENTES.....	14
ATR EN SAM TYPE 4	14
CÓMO OBTENEMOS DEL SAM SU NÚMERO DE SERIE, TIPO Y VERSIÓN.	14
CUAL ES EL PIN DE ACCESO AL SAM DE VALIDACIÓN	15
¿QUE CLAVES HAY QUE UTILIZAR EN EL SAM DE VALIDACIÓN Y EN LA TARJETA DESFIRE?.....	16
¿CÓMO SE REALIZA UNA AUTENTIFICACIÓN?.....	17
3. CÓDIGOS DE RESPUESTA DE UN SAM TIPO 4.....	19

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

1. Comandos del módulo SAM de VALIDACIÓN

1.1. RESET

En principio se resetea el módulo SAM mandando la señal correspondiente en el PIN RST del módulo.

1.2. SELECCIÓN DE APLICACIÓN

Para seleccionar la aplicación del módulo SAM se debe usar este comando, tal y como se detalla.

IMPORTANTE: El tiempo de espera a este comando pondría llegar a ser hasta 500 ms.

COMANDO

CLA	00h
INS	A4h
P1	00h
P2	0Ch
Lc	02h
Datos	1000h

RESPUESTA

90 00	Ejecución del comando correcta.
6A 81	Función no soportada.
6A 82	Fichero no encontrado.
6B 00	Parámetros P1-P2 incorrectos.
6D 00	Código de instrucción no soportado o invalido en el estado de la tarjeta.
6F 00	Problemas internos.

1.3. VERIFICACIÓN PIN (PARA OBTENER CLAVE DE SESIÓN)

El comando para verificar el PIN es:

COMANDO

CLA	00h	
INS	20h	
P1	00h	
P2	07h	Indica en PIN No.7.
Lc	08h	Indica cantidad de Bytes a enviar.
Datos	EF 01 23 45 67 89 AB CD	Representa el PIN 7.

RESPUESTA

90 00	Ejecución del comando correcta.
6A Cx	Verificación de PIN incorrecta. Quedan X intentos.
6B 00	Parámetros P1-P2 incorrectos. P1 ha de ser entre 0 y 11.
6D 00	Código de instrucción no soportado o invalido en el estado de la tarjeta.
6F 00	Problemas internos.

1.4. Obtener respuesta

El comando para obtener la respuesta es:

COMANDO

CLA	00h	
INS	C0h	
P1	00h	
P2	00h	
Lc	XXh	Cantidad de Bytes a recibir.
Datos	Representa la respuesta (los datos a recibir).


	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

1.5. OBTENCIÓN DE CLAVE DE SESIÓN

Para la autenticación con claves de sesión es necesario el uso de dos comandos. En función de la diversificación de clave que se requiera, los comandos tienen unos parámetros u otros.

1.5.1. **OBTENCIÓN DE CLAVE DE SESIÓN – Div. CRTM – 1ª parte**

Este comando de autenticación utiliza la diversificación CRTM para obtener la clave diversificada. El comando para obtener la 1ª parte de la clave de sesión es:

<u>COMANDO</u> 		
CLA	80h	
INS	41h	
P1	01h	
P2	03h	Indica en número de clave.
Lc	15	Indica cantidad de Bytes a enviar.
Le	32	Indica la cantidad de Bytes a recibir.

DATOS A ENVIAR

Los 7 Bytes del número de serie de la tarjeta concatenados por los 8 Bytes de respuesta de la DESFire al mandar el comando de autenticación. O sea, según el manual de DESFire, sección 2.6 (Security Concept): $[SNB0 \dots SNB6 + e_{k_{keyNo}}(RndB)]$.

RESPUESTA

La respuesta tiene dos partes (en total 32 Bytes). Los primeros 16 bytes son el $dk_{keyNo}(RndA+RndB')$ y los segundos 16 bytes son la clave de sesión.

La respuesta se envía mediante el código 61 por lo que se tendrá que recuperar con el comando de “OBTENCIÓN DE RESPUESTA”.

1.5.2. **OBTENCIÓN DE CLAVE DE SESIÓN – Div. CRTM – 2ª parte**

El comando para obtener la 2ª parte de la clave de sesión es:

COMANDO

CLA	80h
INS	41h
P1	02h
P2	00h
Lc	08
Le	00

Indica cantidad de Bytes a enviar.

Indica la cantidad de Bytes a recibir.

DATOS A ENVIAR

Los 8 Bytes de respuesta de la DESFire al mandar el $ekey_{keyNo}(RndA')$.

Atención el parámetro P2 no es fijo, ya que, indica la clave con la que hay que autenticarse.

RESPUESTA

90 00 Ejecución del comando correcta. Quedan XX bytes por leer.

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

1.5.3. **OBTENCIÓN DE CLAVE DE SESIÓN – Div. NXP 2TDEA – 1ª parte**

Este comando de autenticación utiliza la diversificación NXP para obtener la clave diversificada, definida en la nota de aplicación AN10922 para claves 2TDEA.

El comando para obtener la 1ª parte de la clave de sesión es:

COMANDO



CLA 80h

INS 41h

P1 03h

P2 03h

Indica en número de clave.

Lc M + 8

Indica cantidad de Bytes a enviar.

Le 32



Indica la cantidad de Bytes a recibir.

DATOS A ENVIAR

Los M Bytes del Diversification Input (DI) concatenados por los 8 Bytes de respuesta de la DESFire al mandar el comando de autenticación. O sea, según el manual de DESFire, sección 2.6 (Security Concept): $[DIB_0 \dots DIB_{M-1} + ek_{keyNo}(RndB)]$.

NOTA: El DI debe ser UID (7 bytes) || Info Byte (1 byte) || Timestamp (5 bytes), todos ellos obtenidos del FCI en el Select (tal y como se explica en la AN4513).

RESPUESTA

La respuesta son 16 bytes: $dk_{keyNo}(RndA+RndB')$.

La respuesta se envía mediante el código 61 por lo que se tendrá que recuperar con el comando de “OBTENCIÓN DE RESPUESTA”.

1.5.4. **OBTENCIÓN DE CLAVE DE SESIÓN – Div. NXP 2TDEA – 2ª parte**

El comando para obtener la 2ª parte de la clave de sesión es:

COMANDO

CLA 80h

INS 41h

P1 04h

P2 00h

Lc 08

Indica cantidad de Bytes a enviar.

Le 00 

Indica la cantidad de Bytes a recibir.

DATOS A ENVIAR

Los 8 Bytes de respuesta de la DESFire al mandar el $ekey_{keyNo}(RndA')$.

Atención el parámetro P2 no es fijo, ya que, indica la clave con la que hay que autenticarse.

RESPUESTA

La respuesta son los 16 bytes de la clave de sesión.

La respuesta se envía mediante el código 61 por lo que se tendrá que recuperar con el comando de "OBTENCIÓN DE RESPUESTA".

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

1.6. Firma del SAM

Este ejemplo muestra cómo se firma un registro de una transacción tras una validación. Se asume que antes de proceso, se ha realizado una validación de forma exitosa.

Como parámetros de entrada, este proceso requiere:

ClaveSign Índice de la clave del SAM con la que firmar
AFirmar Datos que se desean firmar

Como parámetros de salida, este proceso genera:

Firma Firma resultante.

En este ejemplo vamos a fijar los parámetros de entrada a:

ClaveSign 00h
AFirmar
045F34A9771B8000000001227d4C0B0200000000010010101010016E36198D1
0B771B8601000000000000227D227D4000D101000001h

Ejecutamos directamente el comando de firma.

1. Firma de **AFirmar** con la clave **ClaveSign**.

APDU al SAM. CLA:80h INS:42h P1:00h P2:00h Le:16 Lc:54
DataTx:045F34A9771B8000000001227d4C0B0200000000010010101010016E36198D10B771B8601
000000000000227D227D4000D101000001h
Respuesta. SW: 9000h DataRx: 0424A14Fh

Los 4 bytes de la respuesta son la **Firma**.

Firma =0424A14Fh

1.7. Retrocompatibilidad con los SAM de tipo 4

Los SAM de tipo 4 (en producción en 2018), ofrecen retrocompatibilidad con los SAM actuales (compatible DesFire D40; SAM tipo 1, tipo 2 o tipo 3) en producción. Es decir, funcionan todos los comandos que tenían disponibles los anteriores SAM. Sin embargo, al incorporar familias de claves maestras, es necesario, en algunos casos, conocer cómo se selecciona un conjunto de claves, previo a la autenticación.

Los juegos de claves (o KeySet) agrupan un conjunto de claves que permiten acceder a funcionalidades del sistema de validación del CRTM. Dentro de estas funcionalidades, la principal, es el permitir a los equipos, acceder a los dispositivos sin contacto (tarjetas y móviles).

Cada KeySet da acceso a un conjunto de dispositivos sin contactos, ya sea, físico o virtual.

A continuación, se explica la lógica para determinar, dado un dispositivo sin contactos, que KeySet del SAM se ha de utilizar:

- Si es una tarjeta física DESFire del CRTM cuyo DF tiene como AID = 000001h, se ha de seleccionar el KeySet con Id=0001h
- Si es una tarjeta virtual DESFire del CRTM cuyo DF tiene como AID = 000001h, se ha de seleccionar el KeySet con Id=0005h
- Si es una tarjeta DESFire de EMT cuyo DF tiene como AID = DECADAh, se ha de seleccionar el KeySet con Id=CADAh

El SAM, cuando arranca, por defecto, tiene seleccionado el KeySet con Id=0001h con la versión de claves del CRTM por defecto, es decir, 0000h.

IMPORTANTE: Cada KeySet utiliza 2 bytes para el conjunto de la clave, pero adicionalmente dispone de 2 bytes adicionales para la versión del conjunto de claves

Un SAM de tipo 4 dispone de

- 11 familias de claves del CRTM
- 1 familia EMT

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

1.7.1. **SELECT_KEYSET (instrucción 47h)**

Se selecciona un KeySet de los existentes en el fichero FE_{keys}.

Comando SELECT_KEYSET. Codificación del C-APDU

Campo	Bytes	Valor	Descripción
CLA	1	80h	
INS	1	47h	
P1	1	1 - 2	Modo de selección. Ver Tabla 1
P2	1	00h	RFU
Lc	1	2 ó 4	Cantidad de datos a enviar
Datos Tx	Lc	-	Datos a enviar. Ver Tabla 1

Tabla 1 Comando SELECT_KEYSET. Codificación según P1

Campo	Bytes	Valor	Descripción
P1 = 1, selección de la versión más alta del ID del KeySet indicado			
Lc	1	2	
Datos Tx	Lc	-	- KeySetId (2 bytes)
P1 = 2, selección concreta de KeySet y la versión indicados			
Lc	1	4	
Datos Tx	Lc	-	- KeySetId (2 bytes) - KeySetVers (2 bytes)

Tarjeta física de EMT

EJEMPLO 1: Supongamos que queremos seleccionar el KeySet, para la tarjeta DESFire con AID= DECADAh, tomando el conjunto de claves más alto (es decir, el último). Entonces tendríamos que invocar al SAM de la siguiente forma:

APDU al SAM. CLA:80h INS:47h P1:01h P2:00h Le:0 Lc:2
DataTx: CADAh
Respuesta. SW: 9000h

Tarjetas físicas de CRTM

EJEMPLO 2: Supongamos que queremos seleccionar el KeySet, para la tarjeta DESFire con AID= 000001h, tomando el conjunto de claves más alto (es decir, el último). Entonces tendríamos que invocar al SAM de la siguiente forma:

APDU al SAM. CLA:80h INS:47h P1:01h P2:00h Le:0 Lc:2
DataTx:0001h
Respuesta. SW: 9000h

Tarjetas virtuales de CRTM

EJEMPLO 3: Cuando la tarjeta virtual esté en producción utilizará claves maestras de un KeySet diferente al KeySet utilizado con la DesFire física. Sin embargo, la tarjeta DESFire VIRTUAL, mantendrá el mismo AID que las tarjetas físicas (AID= 000001h). Lo único que cambia es el KeySet en el SAM type 4. El KeySet reservado para las tarjetas virtuales es el 5, por lo que tendríamos que invocar al SAM de la siguiente forma:

APDU al SAM. CLA:80h INS:47h P1:01h P2:00h Le:0 Lc:2
DataTx:0005h
Respuesta. SW: 9000h

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

2. Preguntas frecuentes

ATR en SAM type 4

El ATR, por retrocompatibilidad, es idéntico al de SAMs anteriores excepto en que ha cambiado el *Historical bytes*.

El ATR por defecto contiene:

- Bytes de formato y de información de interfaz.
El valor por defecto es la siguiente secuencia de bytes 3B3E9600h, que indica que solo se puede usar el protocolo T=0 y que el divisor de comunicación mínimo es de 16 clk/ETU. Realmente se puede usar también T=1 e ir hasta 8 clk/ETU, pero no se indica esta posibilidad en el ATR, por retrocompatibilidad.
- Bytes de histórico. Representación en ASCII de "TMI2-SAM ", seguido de los campos SAM_Type y SAM_Version (este último formateado con 3 dígitos), contenidos en el fichero FEap.
Un ejemplo sería "TMI2-SAM 4.001", que lo forman los bytes 544D49322D53414D20342E303031h, donde SAM_Type es 4 y SAM_Version es 1.
- Byte de checksum
Calculo sobre el resto de bytes anteriores. No está presente al solo estar indicado en el ATR el uso de T=0.

Cómo obtenemos del SAM su número de serie, tipo y versión.

Tras haber realizado el reset y haber seleccionado la aplicación

Reset del SAM

ATR=3B3E9600544D49322D53414D20342E303031h

Negociación PPS. T=0, FD=96h


Selección de aplicación 1000h en el SAM

APDU a1 SAM. CLA:00h INS:A4h P1:00h P2:00h Le:0 Lc:2 DataTx:1000h



Respuesta. SW:9000h

hay que leer el número de SAM. Para leer esta información NO HAY QUE PRESENTAR NINGÚN PIN. El comando es el siguiente y lo que hace es leer los 6 primeros bytes del fichero FEap.

	
--	---

CLA 00

INS B0

P1 81

P2 00

Lc 0

Le 6

De los datos devueltos:

SAM_Number: Bytes 1,2 y 3 (ESTE ES EL DATO QUE NOS INTERESA)

SAM_Type: Byte 4

SAM_Version: Byte 5

SAM_Roll: Byte 6

Cual es el PIN de acceso al SAM de validación

El PIN de acceso es el PIN 7: 0x097C818371F493F9

Presentamos el PIN 7 que da permiso a obtener claves de sesión

APDU al SAM. CLA:00h INS:20h P1:00h P2:07h Le:0 Lc:8 DataTx: 097C818371F493F9h

Respuesta. SW:9000h

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

¿Qué claves hay que utilizar en el SAM de Validación y en la tarjeta DesFire?

El SAM de Validación (Type=1, type=2 y type=3) sólo incorpora dos claves: **ReadTransKey** y **ValidTransKey**

Sin embargo, se produce un desfase entre los índices de claves al seleccionarlo en los SAM y en la tarjeta DesFire, pues los índices donde residen las claves ReadTransKey y ValidTransKey varían según esta tabla

nombre de clave	SAM				DesFire
	tipo	version	KeySet	indice Key	indice Key
ReadTransKey		1	x	solo tiene un Set Key3	Key2
ReadTransKey		2	x	solo tiene un Set Key3	Key2
ReadTransKey		3	x	solo tiene un Set Key3	Key2
ValidTransKey		1	x	solo tiene un Set Key4	Key3
ValidTransKey		2	x	solo tiene un Set Key4	Key3
ValidTransKey		3	x	solo tiene un Set Key4	Key3

Por lo tanto, para leer, la autenticación se realiza con la clave 2 (en la tarjeta DesFire) y la clave 3 (en el SAM) y para escribir la autenticación se realiza con la clave 3 (en la tarjeta DesFire) y la clave 4 (en el SAM).

Sin embargo, a partir del SAM de Validación type=4 y versión=2, se incorporan familias de claves, es decir, tendremos varios conjuntos de **ReadTransKey** y **ValidTransKey**. En concreto 11 conjuntos, 11 familias de claves numeradas desde KeySet 0001h hasta el KeySet 000Bh.

Los índices para acceder a **ReadTransKey** y **ValidTransKey**, se seleccionan según el KeySet como indica la tabla:

nombre de clave	SAM				DesFire
	tipo	version	KeySet	indice Key	indice Key
ReadTransKey		4	2	KeySet=0001h Key3	Key2
ReadTransKey		4	2	KeySet>0001h Key1	Key2
ValidTransKey		4	2	KeySet=0001h Key4	Key3
ValidTransKey		4	2	KeySet>0001h Key2	Key3

¿Cómo se realiza una autenticación?

Este ejemplo muestra los pasos a realizar para obtener una clave de sesión de una DESFire usando un SAM type 4.

Como parámetros de entrada, este proceso requiere:

ClaveSam	Es el índice de clave a usar en el SAM dentro del KeySet.
KeySetId	Es el juego de claves de aplicación a usar en el SAM.
ClavePicc	Es el índice de clave a usar la tarjeta RFID.
PIN7	Es el valor del PIN7 del SAM.

Como parámetros de salida, este proceso genera:

ClaveSesión Es la clave de sesión negociada entre el SAM y la DESFire.

En este ejemplo vamos a fijar los parámetros de entrada a:

ClaveSam	03h
KeySetId	0000h
ClavePicc	02h
PIN7	097C818371F493F9h

Empezamos iniciando el SAM. La inicialización del SAM solo se han de hacer una vez.

- Reset del SAM
ATR=3B3E9600544D49322D53414D20342E303031h
Negociación PPS. T=0, FD=96h
- Selección de aplicación 1000h en el SAM
APDU al SAM. CLA:00h INS:A4h P1:00h P2:00h Le:0 Lc:2 DataTx:1000h
Respuesta. SW:9000h
- Presentamos el PIN 7 que da permiso a obtener claves de sesión
APDU al SAM. CLA:00h INS:20h P1:00h P2:07h Le:0 Lc:8 DataTx: 097C818371F493F9h
Respuesta. SW:9000h



Seleccionamos la tarjeta DESFire D40.

- Seleccionar tarjeta DESFire D40
Tarjeta seleccionada. Tipo=DESFire D40. UID=045F34A9771B80h
- Seleccionar aplicación dentro de la DESFire. AID = 000001h
Envío al ctless. Comando=5A000001h
Respuesta=00h

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

Seleccionamos el KeySet adecuado, según el tipo de dispositivo sin contacto y la aplicación seleccionada.

1. Selección del KeySet en el SAM. Se envía el **KeySetId**.

APDU al SAM. CLA:80h INS:47h P1:01h P2:00h Le:0 Lc:2 DataTx:0000h



Respuesta. SW: 9000h

Ahora realizamos la **autenticación entre la tarjeta** (con la clave **ClavePicc**) y el **SAM** (con la clave **ClaveSam**) y obtenemos la clave de sesión.

1. 1ª parte de obtención de clave de sesión con la DESFire D40.

Se envía concatenado 0Ah + **ClavePicc**.

Envío al ctless. Comando=0A02h

Respuesta= AFB89AB17BE255A2BAh

Los últimos 8 bytes de la respuesta son **ekNo(RndB)**.

ekNo(RndB)= B89AB17BE255A2BAh

2. 1ª parte de autenticación con el SAM.

P2=**ClaveSam** y se envía concatenado **DesFireUID** + **ekNo(RndB)**.

APDU al SAM. CLA:80h INS:41h P1:01h P2:03h Le:16 Lc:15
DataTx:045F34A9771B80B89AB17BE255A2BAh

Respuesta. SW: 9000h

DataRx:5D24F092D3D1E621BBE2DEA5C2AD7F58DA244BBE934F45975B7E19C7763144F8h

Los primeros 16 bytes de la respuesta son **dkNo(RndA+RndB')**.

dkNo(RndA+RndB')=5D24F092D3D1E621BBE2DEA5C2AD7F58h

Los últimos 16 bytes de la respuesta son **ClaveSesión**.

ClaveSesión=DA244BBE934F45975B7E19C7763144F8h

3. 2ª parte de obtención de clave de sesión con la DESFire D40.

Se envía concatenado AFh + **dkNo(RndA+RndB')**

Envío al ctless. Comando=AF5D24F092D3D1E621BBE2DEA5C2AD7F58h

Respuesta=001717495B233EE239h

Los últimos 8 bytes de la respuesta son **ekNo(RndA')**

ekNo(RndA')=1717495B233EE239h

4. 2ª parte de autenticación con el SAM.

Se envía **ekNo(RndA')**.

APDU al SAM. CLA:80h INS:41h P1:02h P2:00h Le:16 Lc:8 DataTx: 1717495B233EE239h

Respuesta. SW:9000h

3. Códigos de respuesta de un SAM tipo 4

SW	Descripción
90 00	Ejecución del comando correcta.
61 xx	Ejecución correcta. Se pueden leer xx bytes mediante comando ¡Error! No se encuentra el origen de la referencia..
63 Cx	Verificación del PIN incorrecta quedan x intentos.
67 00	Error de longitud de datos en Lc.
6703	El parámetro P1 es incorrecto.
67 04	El parámetro P2 es incorrecto.
67 05	El fichero .sea es demasiado grande y no cabe en la memoria del SAM.
67 06	El formato del fichero .sea no es correcto.
67 07	La firma con el ID indicado en el fichero .sea no existe.
67 08	La firma con la clave indicada en el fichero .sea no existe.
67 09	El fichero .sea contiene una firma incorrecta.
67 0A	La imagen de SO contiene el CRC incorrecto (puede indicar el descifrado incorrecto).
67 0B	El fichero .sea requiere un algoritmo desconocido para derivar la clave de descifrado.
67 0C	El área de variables de entorno no está inicializado.
67 0D	El sistema de ficheros no está inicializado.
67 0E	El área de variables de entorno ya está inicializado.
67 0F	El sistema de ficheros ya está inicializado.
67 10	El comando requiere una ruta completa, no un filtro.
67 11	El comando no es aplicable a una restricción de acceso (ocurre cuando la variable acaba en '#').

	Área de Innovación Tecnológica	SAM_VALIDACIÓN
542ce224-BIT-NOT-RES-CTM-AIT		

67 12 La ruta de restricción de acceso no es correcta (posiblemente no existe la variable o la ruta).

67 13 El formato de restricción de acceso no es correcto (error en la sintaxis).

67 3D Fallo de autenticación

68 82 Mensajes seguros no soportados.

69 00 Comando no permitido.

69 81 Comando incompatible con la estructura del fichero

69 82 Comando no permitido. Pre-requisitos de seguridad no satisfechos.

69 83 Comando no permitido. Método de autenticación bloqueado.

69 84 Comando no permitido. Dato referenciado no utilizable.

69 85 Comando no permitido. Condiciones de uso no cumplidas.

69 86 Comando no permitido en este FE.

69 87 Comando no permitido. Falta un objeto de datos que se esperaba en el mensaje seguro.

69 88 Comando no permitido. Error en un objeto del mensaje seguro.

6A 00 Error en parámetros P1-P2. Error desconocido.

6A 80 Error en parámetros P1-P2. Parámetros incorrectos en el campo de datos del comando.

6A 81 Error en parámetros P1-P2. Función no soportada.

6A 82 Error en parámetros P1-P2. Fichero o aplicación no encontrado.

6A 83 Error en parámetros P1-P2. Registro no encontrado.

6A 84 Error en parámetros P1-P2. No hay espacio suficiente en el fichero.

6A 85 Error en parámetros P1-P2.

6A 86 Error en parámetros P1-P2. Parámetros P1-P2 incorrectos.

6A 88 Error en parámetros P1-P2. Dato al que se hace referencia en el comando no encontrado.

6A 89 Error en parámetros P1-P2. El fichero ya existe.

- 6A 8A** Error en parámetros P1-P2. El nombre del DF ya existe.
- 6B 00** Parámetros P1-P2 incorrectos.
- 6D 00** Código de instrucción no soportado o inválido en el estado de la tarjeta.
- 6E 00** Clase (CLA) no soportada.
- 6F 00** Problemas internos (error desconocido)